S01P0625

FIG. 1

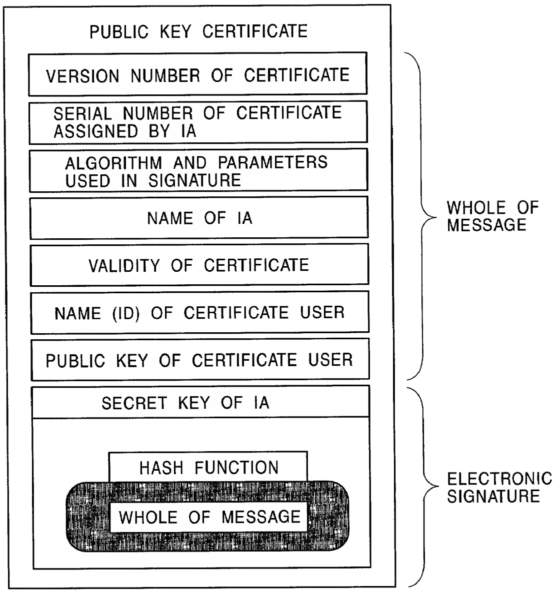


FIG. 2

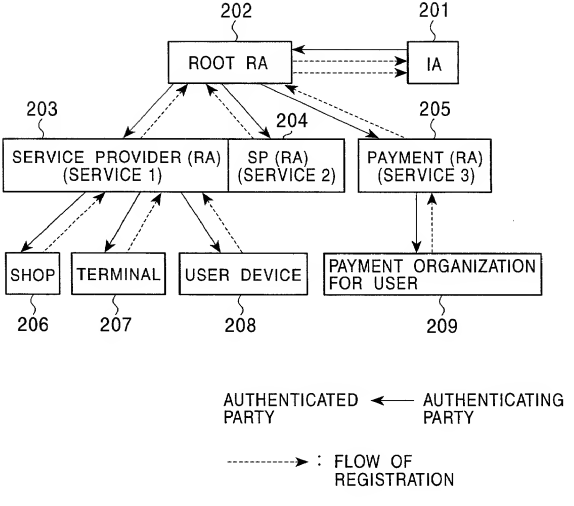

202
201
ROOT RA
IA
203
204
205
SERVICE PROVIDER (RA)
(SERVICE 1)
SP (RA)
(SERVICE 2)
PAYMENT (RA)
(SERVICE 3)
SHOP
TERMINAL
USER DEVICE
PAYMENT ORGANIZATION
FOR USER
206
207
208
209
AUTHENTICATED PARTY ← AUTHENTICATING PARTY
: FLOW OF REGISTRATION

FIG. 3

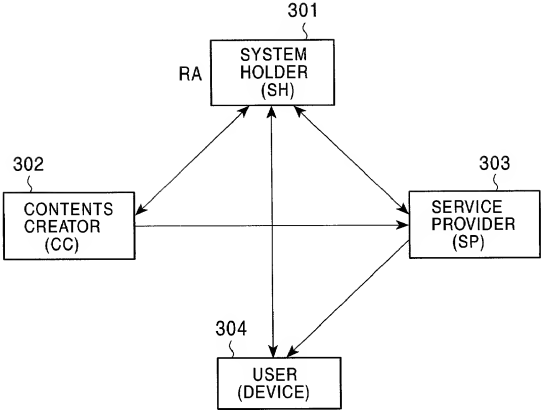

301
SYSTEM HOLDER (SH)
RA
302
CONTENTS CREATOR (CC)
303
SERVICE PROVIDER (SP)
304
USER (DEVICE)

FIG. 4

NO.	SYSTEM HOLDER (SH)	CONTENTS CREATOR (CC)	SERVICE PROVIDER (SP)	USER DEVICE
1.	INTERNET SHOPPING MARKET SPONSOR	MARKETED GOODS PRODUCER AND CONTENTS CREATOR	MARKETED GOODS SHOP	PC
2.	CELLULAR PHONE COMMUNICATION INFRASTRUCTURE PROVIDER	PRODUCER OF CONTENTS AND GOODS PROVIDED USING CELLULAR PHONE INFRASTRUCTURE	CONTENTS DELIVERER TO CELLULAR PHONE USER	CELLULAR PHONE
3.	CABLE-TV CABLE MANAGING ORGANIZATION	CABLE TV PROGRM PRODUCER	CABLE TV COMPANY	TV (SET)
4.	ELECTRONIC MONEY CARD ISSUER	PRODUCER OF CONTENTS AND GOODS PURCHASABLE WITH ELECTRONIC MONEY	ELECTRONIC MONEY AVAILABLE SHOP	IC CARD
5.	- - - - - - - -	- - - - - - - -	- - - - - - - -	- - - -
6.	- - - - - - - -	- - - - - - - -	- - - - - - - -	- - - -

FIG. 5

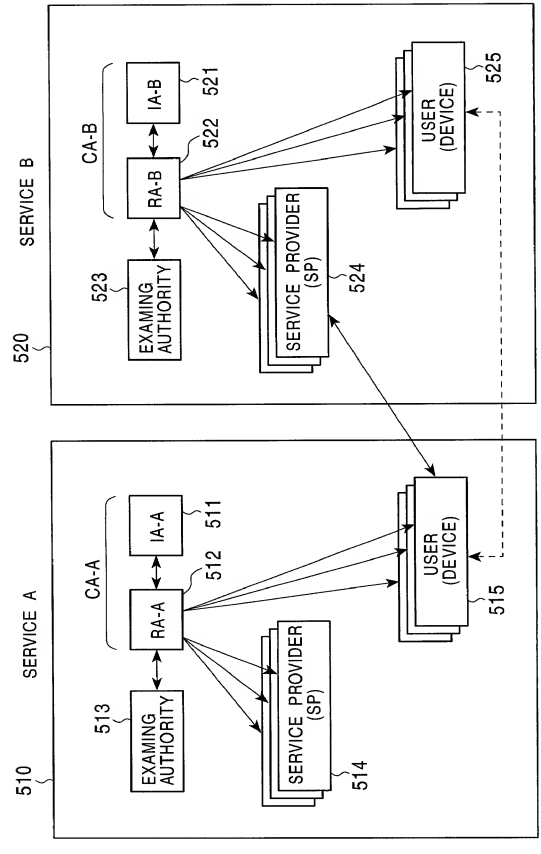

510
SERVICE A
513
EXAMING AUTHORITY
CA-A
RA-A
512
IA-A
511
SERVICE PROVIDER (SP)
514
USER (DEVICE)
515
520
SERVICE B
523
EXAMING AUTHORITY
CA-B
RA-B
522
IA-B
521
SERVICE PROVIDER (SP)
524
USER (DEVICE)
525

FIG. 6

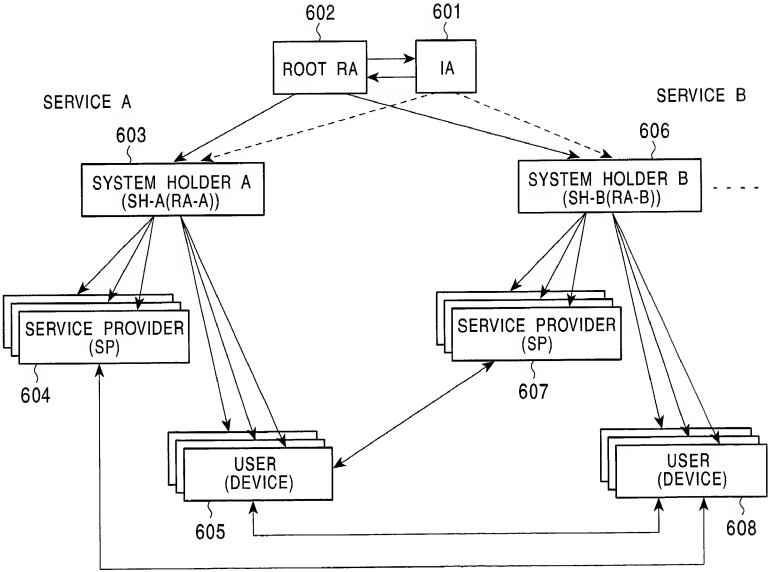


FIG. 7

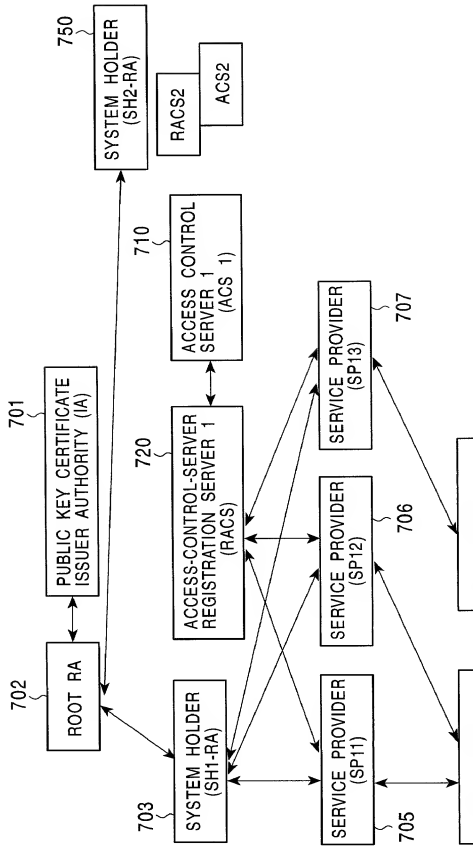

701
PUBLIC KEY CERTIFICATE ISSUER AUTHORITY (IA)
702
ROOT RA
750
SYSTEM HOLDER (SH2-RA)
RACS2
ACS2
710
ACCESS CONTROL SERVER 1 (ACS 1)
720
ACCESS-CONTROL-SERVER REGISTRATION SERVER 1 (RACS)
703
SYSTEM HOLDER (SH1-RA)
SERVICE PROVIDER (SP11)
705
SERVICE PROVIDER (SP12)
706
SERVICE PROVIDER (SP13)
707
USER DEVICE 11
708
USER DEVICE 12
709

FIG. 8

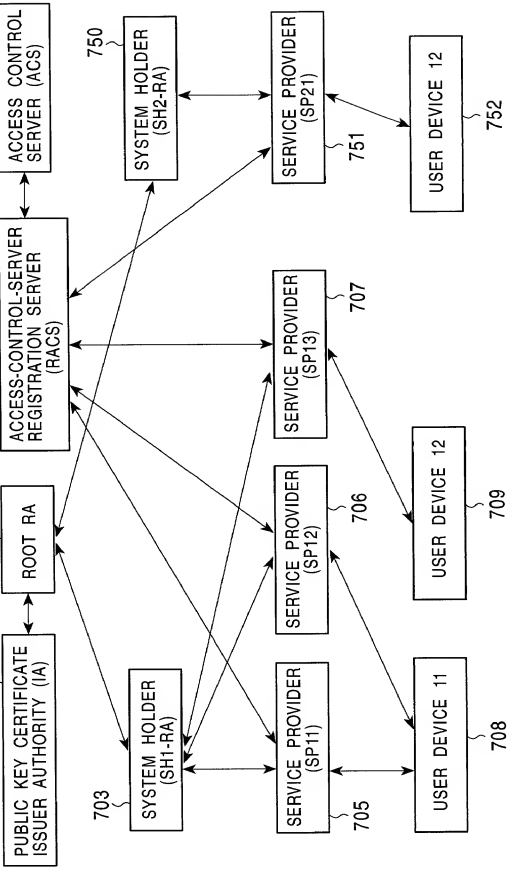

PUBLIC KEY CERTIFICATE ISSUER AUTHORITY (IA)
701
ROOT RA
702
ACCESS-CONTROL-SERVER REGISTRATION SERVER (RACS)
820
ACCESS CONTROL SERVER (ACS)
810
SYSTEM HOLDER (SH1-RA)
703
SYSTEM HOLDER (SH2-RA)
750
SERVICE PROVIDER (SP11)
705
SERVICE PROVIDER (SP12)
706
SERVICE PROVIDER (SP13)
707
SERVICE PROVIDER (SP21)
751
USER DEVICE 11
708
USER DEVICE 12
709
USER DEVICE 12
752

FIG. 9

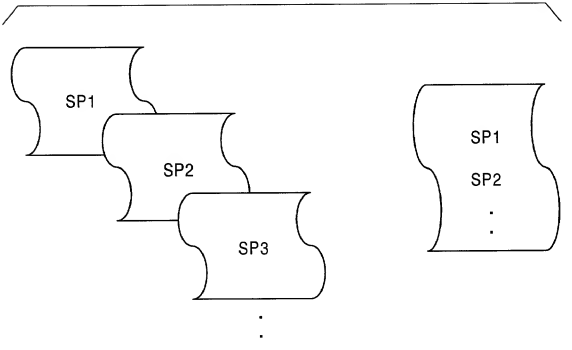


FIG. 10

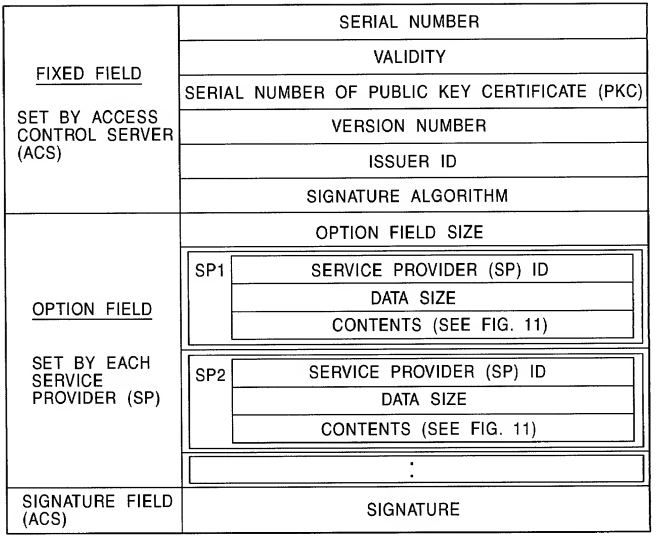

FIXED FIELD
SET BY ACCESS CONTROL SERVER (ACS)
SERIAL NUMBER
VALIDITY
SERIAL NUMBER OF PUBLIC KEY CERTIFICATE (PKC)
VERSION NUMBER
ISSUER ID
SIGNATURE ALGORITHM
OPTION FIELD
SET BY EACH SERVICE PROVIDER (SP)
OPTION FIELD SIZE
SP1
SERVICE PROVIDER (SP) ID
DATA SIZE
CONTENTS (SEE FIG. 11)
SP2
SERVICE PROVIDER (SP) ID
DATA SIZE
CONTENTS (SEE FIG. 11)
SIGNATURE FIELD (ACS)
SIGNATURE

FIG. 11

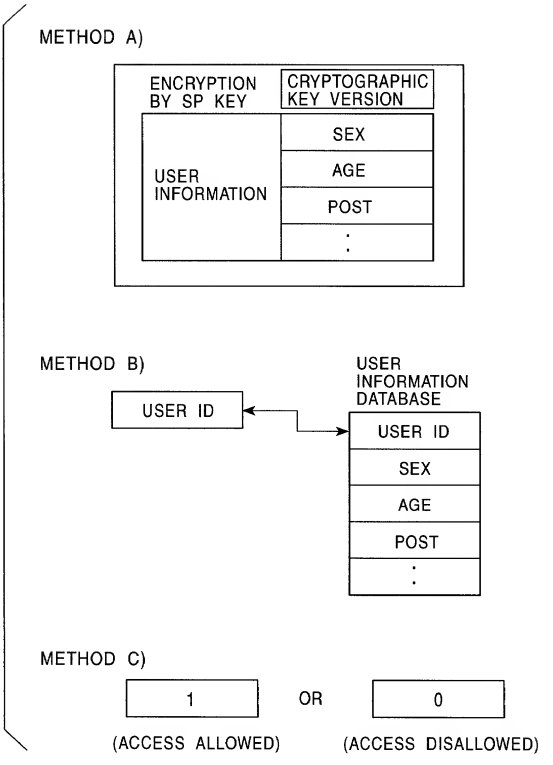

METHOD A)
ENCRYPTION BY SP KEY
CRYPTOGRAPHIC KEY VERSION
USER INFORMATION
SEX
AGE
POST
METHOD B)
USER ID
USER INFORMATION DATABASE
USER ID
SEX
AGE
POST
METHOD C)
1
OR
0
(ACCESS ALLOWED)
(ACCESS DISALLOWED)

FIG. 12

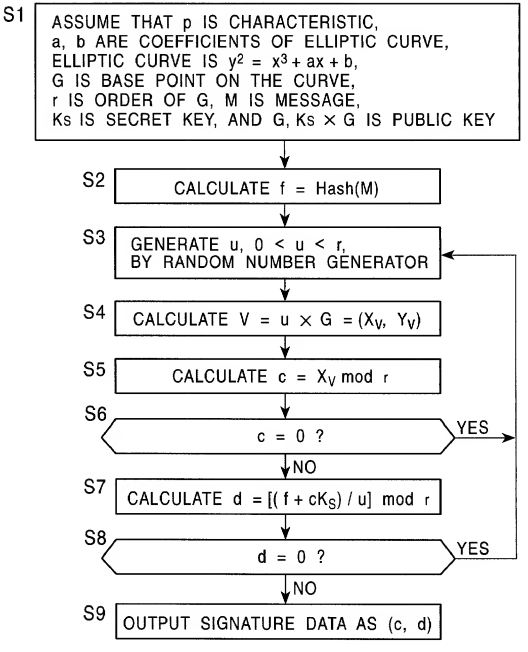

S1
ASSUME THAT p IS CHARACTERISTIC,
a, b ARE COEFFICIENTS OF ELLIPTIC CURVE,
ELLIPTIC CURVE IS $y^2 = x^3 + ax + b$,
G IS BASE POINT ON THE CURVE,
r IS ORDER OF G, M IS MESSAGE,
Ks IS SECRET KEY, AND G, Ks × G IS PUBLIC KEY
S2
CALCULATE f = Hash(M)
S3
GENERATE u, 0 < u < r,
BY RANDOM NUMBER GENERATOR
S4
CALCULATE $V = u \times G = (X_V, Y_V)$
S5
CALCULATE $c = X_V \bmod r$
S6
c = 0 ?
YES
NO
S7
CALCULATE $d = [(f + cK_S) / u] \bmod r$
S8
d = 0 ?
YES
NO
S9
OUTPUT SIGNATURE DATA AS (c, d)

FIG. 13

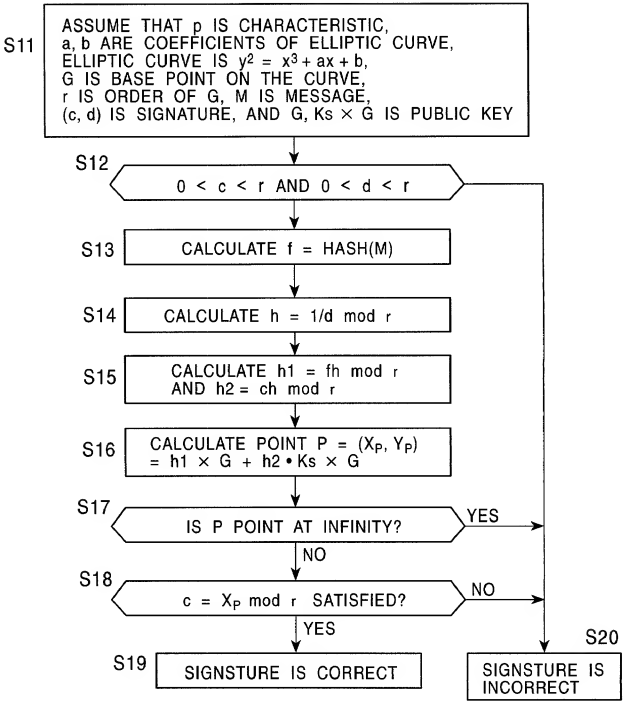

S11
ASSUME THAT p IS CHARACTERISTIC,
a, b ARE COEFFICIENTS OF ELLIPTIC CURVE,
ELLIPTIC CURVE IS $y^2 = x^3 + ax + b$,
G IS BASE POINT ON THE CURVE,
r IS ORDER OF G, M IS MESSAGE,
(c, d) IS SIGNATURE, AND G, Ks × G IS PUBLIC KEY
S12
0 < c < r AND 0 < d < r
S13
CALCULATE f = HASH(M)
S14
CALCULATE h = 1/d mod r
S15
CALCULATE h1 = fh mod r
AND h2 = ch mod r
S16
CALCULATE POINT P = (X_P, Y_P)
= h1 × G + h2 • Ks × G
S17
IS P POINT AT INFINITY?
YES
NO
S18
c = X_P mod r SATISFIED?
NO
YES
S19
SIGNSTURE IS CORRECT
S20
SIGNSTURE IS INCORRECT

FIG. 14

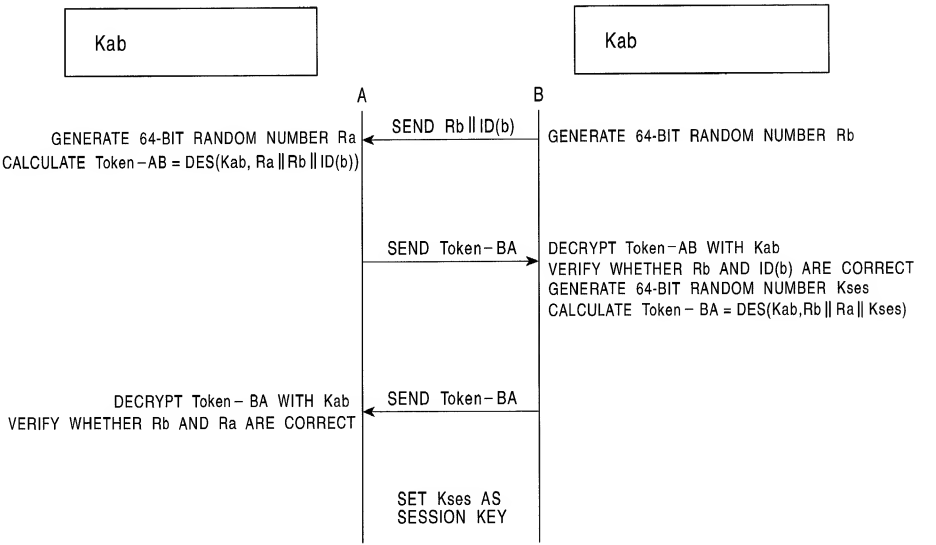


FIG. 15

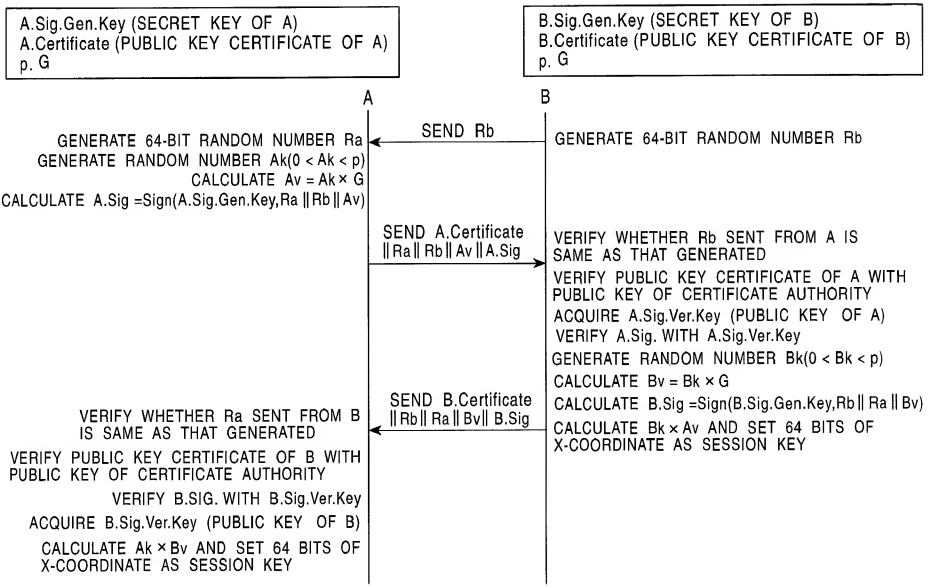


FIG. 16

NO.	TERM	SYMBOL	DESCRIPTION / REMARKS
1	PUBLIC KEY	K_{Pa}	PUBLIC KEY OF A EXAMPLE User → K_{Pa} | UD → K_{Pud} SP → K_{Psp}
2	SECRET KEY	K_{Sa}	SECRET KEY OF A EXAMPLE User → K_{Su} | UD → K_{Sud} SP → K_{Ssp}
3	SESSION KEY	Ks	COMMON KEY CREATED IN MUTUAL AUTHENTICATION
4	CERTIFICATE	A《B》	CERTIFICATE OF B ISSUED BY A EXAMPLE : CERTIFICATE OF UD ISSUED BY IA → IA《UD》
5	ENCRYPTION	E_{Ks}(data)	ENCRYPT PLAINTEXT DATA WITH KEY Ks
6	DECRYPTION	D_{Ks}(data)	DECRYPT CIPHERTEXT DATA WITH KEY Ks
7	SIGNATURE	{data}Sig.K_{Sa}	PUT SIGNATURE TO DATA WITH SECRET KEY K_{Sa} OF A
8	ENCRYPTION WITH SIGNATURE	E_{Ka}({data}Sig.K_{Sa})	PUT SIGNATURE TO DATA WITH SECRET KEY K_{Sa} OF A AND ENCRYPT (DATA ‖ SIGNATURE) WITH KEY K_S

FIG. 17

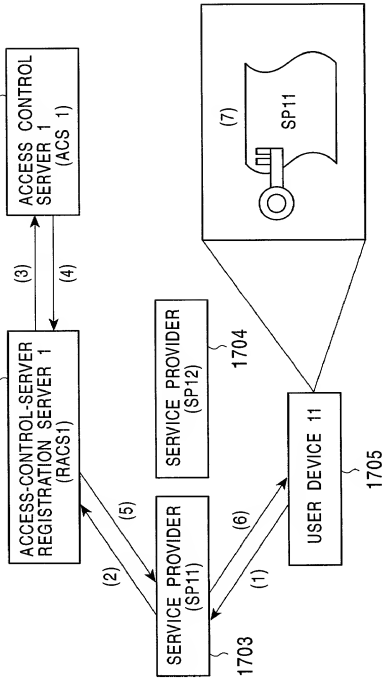

1701
ACCESS CONTROL SERVER 1 (ACS 1)
(3)
(4)
1702
ACCESS-CONTROL-SERVER REGISTRATION SERVER 1 (RACS1)
(2)
(5)
SERVICE PROVIDER (SP11)
1703
SERVICE PROVIDER (SP12)
1704
(6)
(1)
USER DEVICE 11
1705
(7)
SP11

FIG. 18

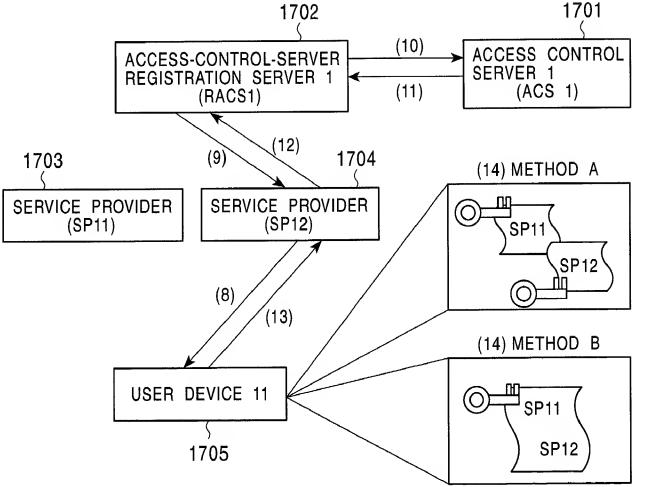


FIG. 19

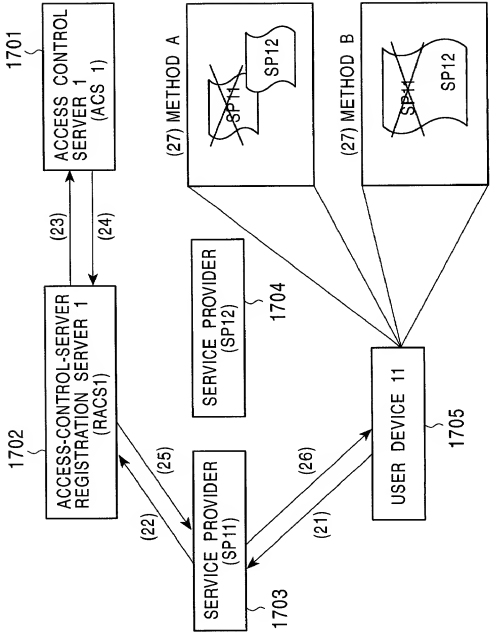

1701
ACCESS CONTROL SERVER 1 (ACS 1)
(23)
(24)
1702
ACCESS-CONTROL-SERVER REGISTRATION SERVER 1 (RACS1)
(22)
(25)
SERVICE PROVIDER (SP11)
1703
SERVICE PROVIDER (SP12)
1704
(26)
(21)
USER DEVICE 11
1705
(27) METHOD A
SP11
SP12
(27) METHOD B
SP11
SP12

FIG. 20

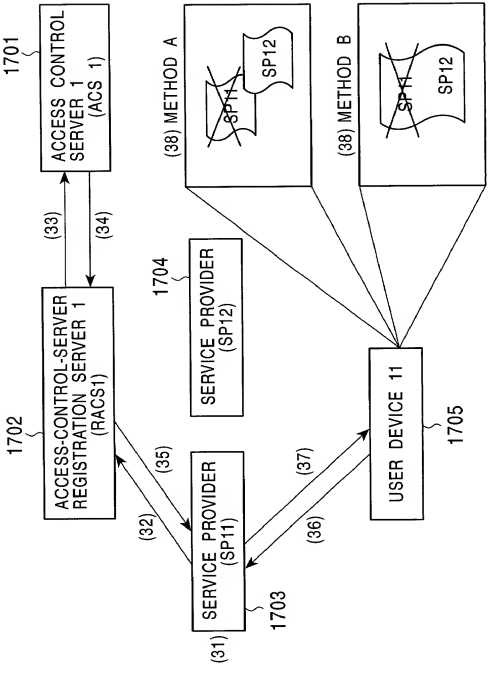

1701
ACCESS CONTROL SERVER 1 (ACS 1)
(33)
(34)
1702
ACCESS-CONTROL-SERVER REGISTRATION SERVER 1 (RACS1)
(32)
(35)
1704
SERVICE PROVIDER (SP12)
(38) METHOD A
SP11
SP12
(38) METHOD B
SP11
SP12
(31)
SERVICE PROVIDER (SP11)
1703
(36)
(37)
USER DEVICE 11
1705

FIG. 21

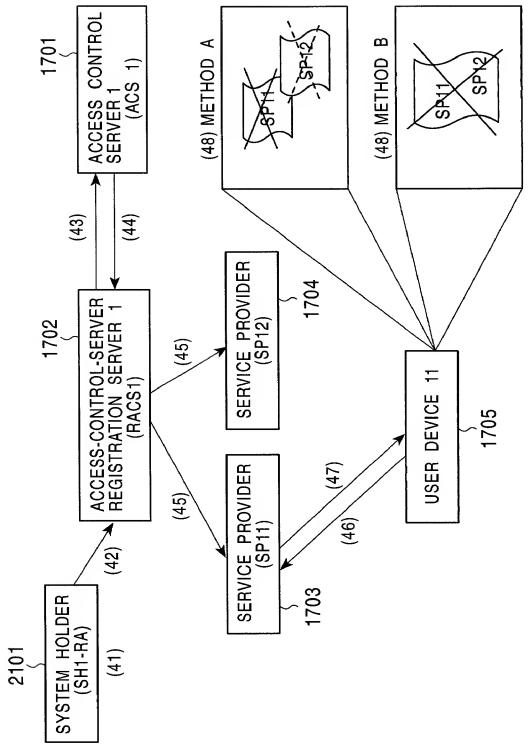

2101
SYSTEM HOLDER (SH1-RA)
(41)
(42)
1702
ACCESS-CONTROL-SERVER REGISTRATION SERVER 1 (RACS1)
(43)
(44)
1701
ACCESS CONTROL SERVER 1 (ACS 1)
(45)
(45)
SERVICE PROVIDER (SP11)
1703
SERVICE PROVIDER (SP12)
1704
(47)
(46)
USER DEVICE 11
1705
(48) METHOD A
SP11
SP12
(48) METHOD B
SP11
SP12

FIG. 22

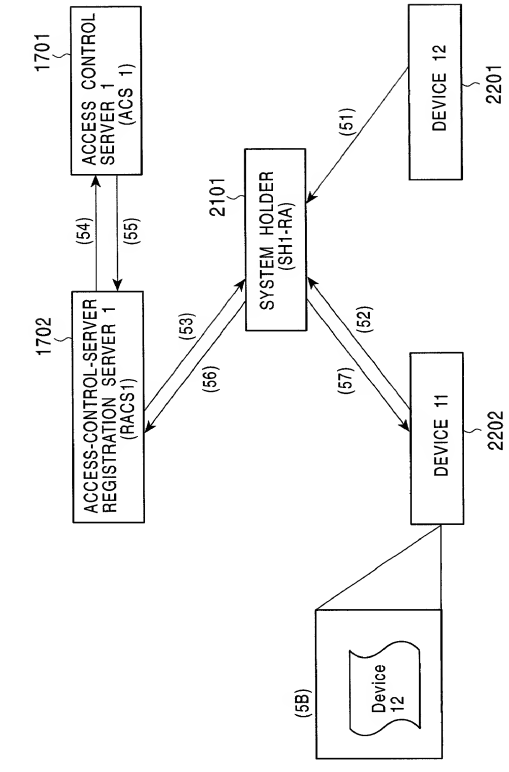

1701
ACCESS CONTROL SERVER 1 (ACS 1)
(54)
(55)
1702
ACCESS-CONTROL-SERVER REGISTRATION SERVER 1 (RACS1)
(53)
(56)
2101
SYSTEM HOLDER (SH1-RA)
(51)
DEVICE 12
2201
(52)
(57)
DEVICE 11
2202
(5B)
Device 12

FIG. 23

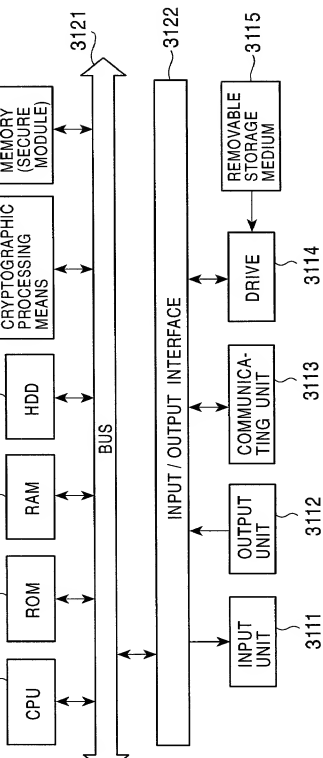
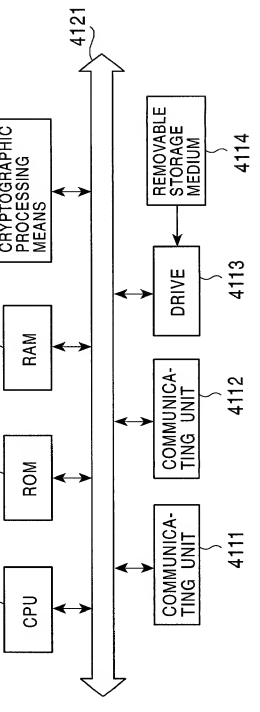

3101
CPU
3102
ROM
3103
RAM
3104
HDD
3105
CRYPTOGRAPHIC PROCESSING MEANS
3106
MEMORY (SECURE MODULE)
3121
BUS
3122
INPUT / OUTPUT INTERFACE
3111
INPUT UNIT
3112
OUTPUT UNIT
3113
COMMUNICATING UNIT
3114
DRIVE
3115
REMOVABLE STORAGE MEDIUM

FIG. 24


4101
CPU
4102
ROM
4103
RAM
4105
CRYPTOGRAPHIC PROCESSING MEANS
4121
COMMUNICA-TING UNIT
4111
COMMUNICA-TING UNIT
4112
DRIVE
4113
REMOVABLE STORAGE MEDIUM
4114